UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

---

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 14-CR-223

STEVEN P. LINK,

Defendant.

---

**DECISION AND ORDER**

---

Defendant Steven P. Link is charged with distribution, receipt and possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) and (a)(5)(B). The charges are based on evidence obtained in a search of his used bookstore in Sturgeon Bay, Wisconsin pursuant to a warrant and the subsequent search of his residence pursuant to the consent of Katherine Johnson, Link's fiancé. The case is before the court on the defendant's motion to suppress both searches. Link seeks suppression of the evidence seized from his bookstore on the ground that the warrant is invalid. He seeks suppression of evidence found on an external hard drive taken during the search of his residence on the grounds that the search exceeded the scope of the consent given by Johnson and, in any event, she lacked authority to provide such consent. For the reasons that follow, Link's motions are denied.

**BACKGROUND**

In or about June of 2014, Lieutenant James Valley of the Brown County Sheriff's Department notified Sergeant Carl Waterstreet of the Sturgeon Bay Police Department that he had downloaded a file containing child pornography from a certain internet protocol (IP) address. (ECF

No. 19, Tr. 44, 74.) An online search revealed that the location of the IP address was Sturgeon Bay and that the service provider was Charter Communications. In response to a communications search warrant, Charter Communications identified the account holder as Steven Link with an address of 18 N. 3rd Avenue, Apartment 2, Sturgeon Bay, Wisconsin, and telephone number of (920) 746-3171. (Ex. 1.) Apartment 2 was directly above a used bookstore located on the first floor in the same building but with an address of 20 N. 3rd Avenue. The website for the bookstore, untitledandrarebooks.com, lists the same telephone number as Apartment 2, and from an online profile, Sergeant Waterstreet learned that Link was the bookstore's "Owner, Chairman, CEO, Board of Directors, Senior and Middle Level Management, Consultant and workforce all wrapped into one person." Using his iPhone on the sidewalk in front of the bookstore, Sergeant Waterstreet detected the presence of a secure wireless network under the name "Untitled Used and Rare." (Tr. 13; Ex. 1.)

Based on this information, Sergeant Waterstreet sought and obtained a search warrant for both Apartment 2 at 18 N. 3rd Avenue and the bookstore at 20 N. 3rd Avenue, which he assumed were connected since they were both under Link's name and shared the same telephone number. Unfortunately, Sergeant Waterstreet failed to include all of the foregoing information in the affidavit he submitted in support of his warrant application and the information he did include was not clearly set forth. For example, Sergeant Waterstreet did not include in his affidavit when Lieutenant Valley had downloaded the file containing child pornography from Link's IP address, nor did he include the name of the secure wireless network he detected on the sidewalk in front of the bookstore. In addition, the paragraph that was apparently intended to describe the connection between the file containing child pornography and the IP address from which it was downloaded lacks clarity. It

reads:

> Your affiant states that during the course of his employment he was notified by Lt. James Valley of the Brown County Sheriff's Office of an Internet Protocol address of 24.196.153.238 for which [sic] became a target of an online child pornography investigation on the Emule network. This Internet Protocol address was associated with MD5 hash value: CB6208424C44450E32C48E598AFD1ADF. A part of this file was identified as being a file of investigative interest to child pornography investigations. A view of the file downloaded is described as:
>
> TITLE: 34 (Sdpa) - Jessica-Christ - 11y - Bro Fuks 11 yo Sis - Ptch.avi. This is a movie of a female under the age of 18 and a male client. The female is on the bed and the male places his penis in her anus multiple times.

(Ex. 1, ¶ 3.)

Upon completing the warrant application, Sergeant Waterstreet took it to the assistant district attorney for her review. The assistant district attorney reviewed the application and indicated her approval. Waterstreet then presented it to a state judge who read over the application and signed the warrant on September 3, 2014.

The warrant was executed on the morning of September 5, 2014. Sergeant Waterstreet met Link outside as he was arriving at the building and gave him a copy of the warrant. Link allowed Sergeant Waterstreet, who was accompanied by other law enforcement officers and a computer forensic analyst from the Division of Criminal Investigations (DCI) of the Wisconsin Department of Justice, into the building where they began searching the bookstore. Several hard drives and two computers were found to contain child pornography as a result of a forensic preview conducted by the analyst from DCI. These items were seized. In addition, Link admitted that he was secretly videotaping people in the basement of the bookstore and in the bathroom, and the agents seized some camera equipment as well.

While searching the book store and in speaking with Link, Sergeant Waterstreet learned that Apartment 2 of 18 N. 3rd Avenue was not connected to the bookstore and that the current occupant was Kory Murphy. Murphy was present in the apartment when Sergeant Waterstreet and the officers assisting him proceeded to that location after they completed his search of the bookstore. In the course of their search of the apartment, the officers located two laptops, some video cameras and cell phones on which the forensic preview disclosed the presence of child pornography. Based on this evidence, Murphy was later charged separately from Link. It does appear, however, that the two shared the same internet access. While searching the apartment, Sergeant Waterstreet observed a cable running from a modem through a hole in the floor to the bookstore where it was connected to a wireless router. No router was found in the apartment occupied by Murphy.

Later that day, Sergeant Waterstreet proceeded with the other officers to a residence Link shared with Katherine Johnson, his fiancé. Johnson operated a daycare out of their residence, and Waterstreet was concerned that Link may have set up hidden cameras in the home or otherwise placed the children at risk. Upon arrival at the home, Sergeants Waterstreet and Zager identified themselves and asked Ms. Johnson for permission to search. They told her that they had discovered child pornography on Link's computers at the bookstore and that he had admitted that he had secretly videotaped people with hidden cameras. They asked if they could come in and look for computers that may contain child pornography and any cameras. Stating she had nothing to hide, Johnson allowed them into the house and led them to the bedroom she shared with Link.

Johnson showed them two computers with external hard drives located on a wire-like stand in the closet. Johnson stated that the computers belonged to Link but explained that the computers were used to display shows downloaded from the internet on the television set. While Sergeant

Waterstreet and another officer looked for hidden cameras, Sergeant Zager remained in the bedroom with the computers. Sergeant Zager explained to Johnson that he wanted to remove the internal hard drives from the computers and take them outside to their van so that the DCI agent could do a quick preview to determine whether they contained child pornography. He told her he would bring them back into the house and put them back into the computers if no child pornography was found. Although Sergeant Zager could not recall what if anything Johnson said in response, she indicated she had no objection. Sergeant Zager also took the external hard drives outside to be searched as well. These also belonged to Link. Johnson continued to cooperate with the officers even after child pornography was found on one of the external hard drives and even after Link telephoned and spoke with her from the jail. (Tr. 86-88.)

At the hearing on Link's motion to suppress, Johnson explained that she didn't know that one of the external hard drives, the one on which the child pornography was found, was even at the house. She explained that Link usually would take that hard drive back and forth to work with him. She explained that they did not have internet access at home, and so Link would download shows, music or documentaries at work and bring it home so they could watch it on their television. Johnson testified that the hard drive belonged to Link and that she never accessed it. She testified she didn't know much about computers and would generally watch DVDs with her child, though she also admitted that the computers were not password protected. She stated she had no idea that Sergeant Zager was removing the hard drives and taking them outside to search them and specifically denied giving permission to search the external drive that Link took back and forth to work since she didn't even know it was there.

## I. SEARCH WARRANT FOR BOOKSTORE

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures...." U.S. Const. amend. IV. When a search is authorized by a warrant, "great deference" is given to the issuing judge's conclusion that probable cause has been established. *United States v. Garcia*, 528 F.3d 481, 485 (7th Cir. 2008). A search warrant affidavit establishes probable cause when "it sets forth sufficient evidence to induce a reasonably prudent person to believe that a search will uncover evidence of a crime." *United States v. Mykytiuk*, 402 F.3d 773, 776 (7th Cir. 2005) (internal quotations omitted). "[T]he task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him, ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Koerth*, 312 F.3d 862, 866 (7th Cir. 2002). An issuing magistrate "is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense." *United States v. Orozco*, 576 F.3d 745, 749 (7th Cir. 2009). "[I]n reviewing the issuing judge's probable cause determination, the district court need only evaluate whether the judge had a 'substantial basis' for concluding that probable cause existed." *United States v. Kelly*, 772 F.3d 1072, 1080 (7th Cir. 2014) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

Link argues that the affidavit submitted by Sergeant Waterstreet fails to establish probable cause. He contends that paragraph three of the affidavit, the only paragraph that even purports to connect child pornography to an IP address associated with Link, is "so cryptic and confusing as to be nearly incomprehensible." (ECF No. 21 at 5.) Link notes that the affidavit states that Sergeant Waterstreet was notified by Lieutenant Valley of an IP address that "became the target of an online

child pornography investigation on the Emule network." No explanation is given, however, as to how the IP address became a target of an investigation, why it became a target, or even who determined it was a target. The affidavit also fails to explain what an Emule network is or why that fact is significant. The paragraph goes on to say that the IP address was associated with a particular MD5 hash value, but does not explain what is meant by "associated with" or what an MD5 hash value is or who made this determination. The paragraph then refers to a "file" and states that "a part of this file was identified as being a file of investigative interest to child pornography investigations," but fails to say why the file was of investigative interest and what being of investigative interest means. Finally, the paragraph includes a description of "a view of the file downloaded" but fails to say who viewed the file and is offering the description.

The problem is compounded by the facts that there is no indication when the file was downloaded from the listed IP address, assuming it was downloaded from that IP address, and the location shown for the IP address is an apartment on the second floor of 18 N. 3rd Avenue, yet the warrant authorizes a search of a book store which, while in the same building, is located on the first floor and has a separate address. Link contends that there is no evidence in the affidavit that the bookstore has internet access or contains computers or other devices that can access the internet. The fact that Sergeant Waterstreet detected a secure wifi network on the sidewalk in front of the bookstore, absent evidence that the store was connected to the network, is irrelevant. And because the affidavit fails to state when the IP address "was associated with" the file containing child pornography or when the file was downloaded from that IP address, there is no basis for concluding that evidence of the crime would still be there. In other words, there is no reason to believe the evidence was not stale.

The government concedes, as it must, that the affidavit could have been better written, but argues that it is nevertheless sufficient to establish probable cause. While not a model of clarity, the government argues that a common sense reading of the affidavit leads to the conclusion that in the course of a child pornography investigation, law enforcement had downloaded a digital file containing child pornography from a particular IP address for a computer located in Apartment 2 of 18 N. 3rd Avenue in Surgeon Bay, Wisconsin. Charter Communications, the internet service provider, identified Link at the same address as the account holder. The affidavit also identified Link as the sole owner/operator of a used book store located in the same building directly below the apartment. In addition to the same occupant or owner, both the bookstore and the apartment also shared the same telephone number, suggesting that they were connected to each other. Finally, the affidavit noted that the bookstore had its own website, untitledandrarebooks.com, which at least suggested that it had an internet presence, and included Link's online profile at a social media site in which he describes himself as a former Charter Communications Divisional Operations Analyst capable of getting "any raw data format he wanted out of any database regardless of complexity."

The government's reading of the affidavit is not a common sense reading. Instead, it is a reading informed by technical knowledge of how child pornography investigations are conducted that allows it to cut through the cryptic jargon Sergeant Waterstreet employed in his affidavit and make sense out of what otherwise one might find hopelessly confusing. For this reason alone, I conclude that probable cause was lacking. Moreover, having failed to indicate when the file containing child pornography was downloaded from Link's IP address, it is impossible to determine whether the evidence was stale. The Seventh Circuit has noted that it is rare that evidence of child pornography being uploaded to or downloaded from a computer will be stale. This is because "[c]omputers and

computer equipment are 'not the type of evidence that rapidly dissipates or degrades.'" *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012) (quoting *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010)). Still, with evidence of only a single download and no indication when it occurred set forth in the affidavit, no probable cause was shown. *See United States v. Prideaux-Wentz*, 543 F.3d 954, 959 (7th Cir. 2008) ("The four year gap, without more recent evidence, undermines the finding that there was probable cause that the images would be found during the search. Therefore, we find that the evidence relied on to obtain the warrant here was stale, and the warrant lacked probable cause.").

A further problem with the warrant was the lack of a nexus between the evidence sought—the child pornography, and the bookstore owned by Link. It is true that Link was both the owner of the account with the internet service provider and the bookstore. But the IP address linked to the child pornography was for an account with a billing address of 18 N. 3rd Avenue, Apartment 2, Sturgeon Bay, Wisconsin. An IP addresss is unique to a specific computer and is generally considered a fairly unique identifier so that it can ordinarily be relied upon to show probable cause as to the residence to which the IP address was assigned. *United States v. Vosburgh*, 602 F.3d 512, 526 (3d Cir. 2010) (noting that courts have held that "evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address"). Here, the government argues that because Link was both the owner of the account and the owner of the bookstore, a wifi network was detected immediately outside the bookstore, and because both the apartment and the bookstore had the same telephone number, a sufficient nexus was shown, especially given Link's claimed knowledge and experience as a former Charter Communications Divisional Operations Analyst.

Regardless of whether a sufficient nexus was shown to establish probable cause, I conclude that the showing is at least sufficient to support the finding necessary for the application of the good faith exception to the exclusionary rule under *United States v. Leon*, 468 U.S. 897, 920–24 (1984). That Sergeant Waterstreet acted in good faith is clear. "An officer's decision to obtain a warrant is prima facie evidence that he or she was acting in good faith." *United States v. Olson*, 408 F.3d 366, 372 (7th Cir. 2005) (citing *Koerth*, 312 F.3d at 868). The fact that Sergeant Waterstreet also had the warrant application reviewed by an assistant district attorney before presenting it to the judge further supports a finding that he was acting in good faith. *See United States v. Pappas*, 592 F.3d 799, 802 (7th Cir. 2010) ("Consulting 'with the prosecutor prior to applying for [a] search warrant provides additional evidence of [that officer's] objective good faith.'") (quoting *United States v. Bynum*, 293 F.3d 192, 198 (4th Cir.2002)).

A defendant may rebut the prima facie evidence of good faith by presenting evidence to establish that:

> (1) the issuing judge wholly abandoned his judicial role and failed to perform his neutral and detached function, serving merely as a rubber stamp for the police; (2) the affidavit supporting the warrant was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or (3) the issuing judge was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.

*United States v. Elst*, 579 F.3d 740, 744 (7th Cir. 2009). Here, despite the sparse detail and poor quality of the affidavit, there is no evidence from which Sergeant Waterstreet could have concluded that the judge had abandoned his judicial role and failed to perform his neutral and detached function by serving merely as a rubber stamp. The undisputed testimony is that the judge reviewed the affidavit and warrant, asked no questions, and signed it. And this occurred after the assistant district

attorney had previously reviewed and approved the application. The exclusionary rule is intended to deter police misconduct, not that of prosecutors and judges. *Leon*, 468 U.S. at 916. Given the fact that both approved the warrant in this case, Sergeant Waterstreet cannot be faulted for acting in reliance upon it.

I likewise conclude that the affidavit is not so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable. While, as noted above, the government's reading of the affidavit is not a common sense reading, it is a reasonable reading taking into account the technical aspects of how child pornography investigations are conducted. Indeed, no other reading makes sense, and the testimony at the hearing on Link's motion confirmed that the government's reading was factually accurate. In June 2014, Lieutenant Valley of the Brown County Sheriff's Department downloaded the video file described in the affidavit from a computer with the stated IP address. Sergeant Waterstreet viewed the file, confirmed that it constituted child pornography, and obtained a communications search warrant that identified Link of 18 N. 3rd Avenue, Apartment 2, in Sturgeon Bay as the holder of the account for that IP address. Because Link was also the sole owner/operator of the bookstore located in the same building directly under Apartment 2, and the bookstore shared the same telephone number as Apartment 2, Sergeant Waterstreet reasonably assumed that Apartment 2 served as an office or was otherwise connected to the bookstore. The name of the secure wifi network was strong evidence that Link also had internet access through the bookstore, likely through the same account. Even the failure to include the date the material was downloaded in the warrant was not so clearly fatal to its validity that it can be said Sergeant Waterstreet did not reasonably rely on the warrant. *See United States v. Summage*, 481 F.3d 1075, 1078 (8th Cir. 2007) (holding that failure to include in affidavit the date on which photos of child

were taken not fatal to a determination that probable cause existed for a search of defendant's new residence). For these reasons, Sergeant Waterstreet's reliance on the warrant was not unreasonable such that the exclusionary rule should apply.

Link does not even argue that the issuing judge was misled by information contained in the affidavit that the affiant knew or should have known was false. It thus follows that the third exception to the good faith exception is also inapplicable. Accordingly, despite the fact that the affidavit failed to establish probable cause, I conclude that Sergeant Waterstreet acted in good faith reliance upon the warrant in his search of the bookstore. Link's motion to suppress evidence obtained in that search is therefore denied.

## II. CONSENT TO SEARCH OF DEFENDANT'S HOUSE.

There is no dispute that Johnson gave police consent to enter the residence she shared with Link to look for hidden video cameras and to look for child pornography on the two computers in the bedroom she shared with him. The dispute is over whether Johnson gave the officers consent to search Link's external hard drive on which they discovered child pornography and, if so, whether Johnson had authority to give such consent, whether actual or apparent. Because consent is an exception to the requirement for a search warrant, the government has the burden of proving both that such consent was given and that it was voluntary. *United States v. Beltran*, 752 F.3d 671, 679 (7th Cir. 2014).

Though the testimony was conflicting in some areas, it was for the most part consistent. Based upon the testimony, I find that Johnson consented to the entry of the law enforcement officers into the home she shared with Link to search for hidden cameras and for child pornography.

Johnson led Sergeant Zager to the bedroom she shared with Link and pointed to the two computers on a stand in the closet. An external hard drive was either on top of or lying next to each computer on the stand. Although Johnson testified that she did not realize that Sergeant Zager was removing the internal hard drives and taking them, along with the external hard drives, outside for a forensic preview, I find Sergeant Zager's testimony that he told her what he was doing and she observed him taking them outside more convincing.

The first issue here concerns the scope of the consent. Did the consent given by Johnson extend to allowing Sergeant Zager to remove the hard drives from the computer and take them, along with the external hard drives, out to the DCI van so that a forensic preview could be quickly conducted? "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?" *Florida v. Jimeno*, 500 U.S. 248, 251 (1991) (quoting *Illinois v. Rodriguez*, 497 U.S. 197, 183-189 (1990)). Moreover, "[t]he scope of a search is generally defined by its expressed object." *Id.* (citing *United States v. Ross*, 456 U.S. 798 (1982)). Here, the officers asked for and were given consent to search the computers for child pornography. Absent some limitation, a reasonable police officer would believe that the consent given by Johnson authorized them to search where child pornography would reasonably be located, namely, on a computer's hard drive, whether internal or external. *See United States v. Anderson*, 533 Fed.Appx. 668 (7th Cir. 2013) (holding that consent to search for evidence of sexual assault extended to computer and storage media). Sergeant Zager was confirmed in this belief when he explained to Johnson that he intended to remove the internal hard drives from the computers and take them outside to the van where they would perform a quick preview and she interposed no

objection. *See United States v. Jackson*, 54 Fed.Appx. 870, 872 (7th Cir. 2002) ("We have repeatedly held that a person's failure to object to an ongoing search undermines a later challenge that the search was conducted without consent.") (citing *United States v. Saadeh*, 61 F.3d 510, 518-19 (7th Cir.1995)). Johnson likewise did not object when he proceeded to do just that. Johnson's failure to object or limit Sergeant Zager's search was consistent with her response that she had nothing to hide and her cooperative attitude throughout the search. I conclude that Johnson's consent to search the computers for child pornography was broad enough to cover the search of both the internal and external hard drives conducted by police.

The closer question is whether Johnson had authority to consent to such a search. On this issue, too, the government has the burden of proof. *United States v. James*, 571 F.3d 707, 714 (7th Cir. 2009) ("The government has the burden of proving authority to consent by a preponderance of the evidence."). The general rule is that "the consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared." *United States v. Matlock*, 415 U.S. 164, 170 (1974). The common authority needed to justify third-party consent "rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." Id. at 171 n.7. Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses authority to consent. *See Georgia v. Randolph*, 547 U.S. 103, 109 (2006).

Here it is clear that Johnson lived at the residence with Link and shared the bedroom in which the computers were located. But Johnson was more than a tenant; she was Link's fiancé, the mother of his four-year-old child with whom he shared not only a home but his bed. *See United States v. Robinson*, 479 F.2d 300, 303 (7th Cir. 1973). Although the computers were owned by Link, this fact is not determinative. The "common authority [needed for third party consent] rests 'on mutual use of the property by persons generally having joint access or control for most purposes.'" *United States v. Duran*, 957 F.2d 499, 503 (7th Cir. 1992). It is also not determinative that Johnson did not often use the computers or hard drives. The issue is whether she had joint access, not whether she used such access. *Id.* at 505 ("Accordingly, the mere fact that Karen neither used the old farmhouse nor left any of her personal effects there does not bear on whether Cesar maintained exclusive dominion over the structure. One can have access to a building or a room but choose not to enter.").

This is not to say that a spouse or live-in fiancé has authority to consent to any search that occurs within a shared home. "When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object." *United States v. Andrus*, 483 F.3d 711, 717 (10th Cir. 2007). Certain objects and containers, such as valises, suitcases, footlockers, and strong boxes, are typically associated with high expectations of privacy. *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978). Computers have been held to fall into this category. *United States v. Stabile*, 633 F.3d 219, 232-33 (3d Cir. 2011); *Andrus*, 483 F.3d at 718; *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001). Where the owner of such a highly personal object has indicated a subjective expectation of privacy by locking the container or otherwise rendering it inaccessible to a co-occupant of the premises, the common authority over the object

required for third party consent will not be found. *See, e.g.,United States v. Block*, 590 F.2d 535, 537 (1978) (holding mother lacked authority to consent to search of son's footlocker where "[t]he trunk was fastened shut by some means that indicated to the officers that it was locked and that a key was required to open it"). In the computer context, a subjective expectation of privacy is manifest by protecting one's files with a password. *Stabile*, 633 F.3d at 232; *Andrus*, 483 F.3d at 719; *Truloch*, 275 F.3d at 403. The failure to use password protection suggests that the defendant "assumed the risk" that the other person would consent to its search. *United States v. King*, 604 F.3d 125, 137 (3d Cir.2010) (quoting *Matlock*, 415 U.S. at 171 n.7); *see also Stabile*, 633 F.3d at 233 ("The failure to use password protection indicates that Stabile relinquished his privacy in the contents of the computer.").

Based upon these considerations, I conclude that Johnson had actual authority to consent to the search of Links computers and hard drives. Having left the equipment in the common area he shared with her and having failed to use password protection, Link gave Johnson common access to the equipment and assumed the risk that she would consent to its search by others. Not only did he not protect his privacy with a password, but the record reflects the absence of any instructions Link gave Johnson that would have led her to believe her access was limited. By leaving the computers and the external hard drives that contained the movies and shows they would watch in the bedroom he shared with her, Link relinquished any expectation of privacy he otherwise might have had in those devices as to Johnson.

Alternatively, Sergeant Zager had at least apparent authority to search the hard drives. Johnson shared the residence with Link and indicated that she used the computers with him to watch television shows that were downloaded from the internet. She offered no objection when he

explained how he intended to conduct the search to which she had already consented, and again offered no objection as he carried the hard drives out to the DCI van to conduct the preview. Based on this evidence, it was reasonable for Sergeant Zager to believe that Johnson possessed the authority to consent.

Finally, in the event Johnson lacked even apparent authority to consent to the search of the hard drives, the fruits of the search would nevertheless be saved under the inevitable discovery doctrine. "Under the inevitable discovery doctrine, illegally seized evidence need not be suppressed if the government can prove by a preponderance of the evidence that the evidence inevitably would have been discovered by lawful means." *United States v. Pelletier*, 700 F.3d 1109, 1116 (7th Cir. 2012) (citing *Nix v. Williams*, 467 U.S. 431, 442–44 (1984)). For the inevitable discovery doctrine to apply, the government must show (1) "that it had, or would have obtained, an independent, legal justification for conducting a search that would have led to the discovery of the evidence"; and (2) "that it would have conducted a lawful search absent the challenged conduct." *United States v. Marrocco*, 578 F.3d 627, 637–38 (7th Cir. 2009). In *Pelletier*, the Court affirmed the denial of a motion to suppress evidence of child pornography on the ground that even if the defendant's consent to the search of his computer was involuntary, the evidence discovered during the search would have been discovered anyway because the law enforcement officers would have obtained a search warrant for the computer. The same is true here.

If Johnson had told Sergeants Waterstreet and Zager that she did not have authority to consent to the search of the hard drives, it is clear they would have sought and obtained a search warrant for at least the external hard drive that he generally took to the book store. By the time they spoke with Johnson, Sergeants Waterstreet and Zager knew that child pornography had been

discovered on Link's bookstore computers and that he had been secretly videotaping people in the basement and bathroom of his store. As someone with training in the investigation of child pornography crimes, Sergeant Waterstreet would have known that those who commit such crimes often keep it on multiple media formats. *See United States v. Anderson*, 533 Fed. Appx. 668, 671 (7th Cir. 2013) (noting that "digital media have become so ubiquitous in the 21st century that rarely will storage devices not be 'pertinent' in an investigation of the sexual assault of a child"). Indeed, had Link taken the external hard drive with him to work as he typically did, it would have fallen well within the scope of the search that had already been authorized. Under these circumstances, I conclude that even if Johnson's consent was invalid, the motion should be denied.

**ORDER**

Accordingly, and for the reasons set forth above, the defendant's motion to suppress the evidence obtained as a result of the search of the bookstore and his residence is denied.

Dated at Green Bay, Wisconsin, this 18th day of February, 2015.

s/ William C. Griesbach
WILLIAM C. GRIESBACH, Chief Judge
United States District Court - WIED